

# A VARIANT OF THE BOMBIERI-VINOGRADOV THEOREM IN SHORT INTERVALS WITH APPLICATIONS

JESSE THORNER

**ABSTRACT.** We generalize the classical Bombieri-Vinogradov theorem to a short interval, non-abelian setting. This leads to variants of the prime number theorem for short intervals where the primes lie in arithmetic progressions that are “twisted” by a splitting condition in a Galois extension  $L/K$  of number fields. Using this result in conjunction with recent work of Maynard, we prove that rational primes in short intervals with a given splitting condition in a Galois extension  $L/\mathbb{Q}$  exhibit dense clusters in short intervals. We explore several arithmetic applications related to questions of Serre regarding the nonvanishing Fourier coefficients of cuspidal modular forms, including finding dense clusters of fundamental discriminants  $d$  in short intervals for which the central values of  $d$ -quadratic twists of modular  $L$ -functions are non-vanishing.

## 1. INTRODUCTION AND STATEMENT OF RESULTS

Let  $\mathbb{N}$  denote the set of positive integers, and let  $a, q \in \mathbb{N}$  satisfy  $(a, q) = 1$ . Define

$$\psi(x; q, a) = \sum_{\substack{n \leq x \\ n \equiv a \pmod{q}}} \Lambda(n),$$

where  $\Lambda(n)$  is the von Mangoldt function. The prime number theorem for arithmetic progressions tells us that if  $q \leq (\log x)^D$  for any constant  $D > 0$ , we have

$$(1.1) \quad \psi(2x; q, a) - \psi(x; q, a) \sim \frac{x}{\varphi(q)},$$

where  $\varphi$  denotes Euler’s totient function. Understanding both the error term and the range of  $q$  for (1.1) is important for a wide variety of arithmetic problems. The Generalized Riemann Hypothesis (GRH) for Dirichlet  $L$ -functions implies that if  $q \leq x^{1/2-o(1)}$ , then

$$(1.2) \quad \psi(2x; q, a) - \psi(x; q, a) - \frac{x}{\varphi(q)} \ll \sqrt{x}(\log qx)^2.$$

While this is beyond the reach of current methods, it is known that the mean value of (1.2) is about as small as predicted by GRH when we average over moduli  $q$ . More specifically, if  $0 \leq \theta < \frac{1}{2}$  is constant, Bombieri and Vinogradov proved that for any fixed  $D > 0$ , we have

$$(1.3) \quad \sum_{q \leq x^\theta} \max_{(a,q)=1} \max_{N \leq x} \left| \psi(2N; q, a) - \psi(N; q, a) - \frac{N}{\varphi(q)} \right| \ll \frac{x}{(\log x)^D}.$$

A more difficult problem asks for the distribution of primes in arithmetic progressions when the interval  $[x, 2x]$  is replaced with  $[x, x+h]$ , where  $h \geq x^{1-\delta}$  for some  $\delta > 0$ . Using

deep analytic properties of Dirichlet  $L$ -functions, one can produce a short interval analogue of the Bombieri-Vinogradov estimate (1.3) of the form

$$(1.4) \quad \sum_{q \leq x^\theta} \max_{(a,q)=1} \max_{y \leq h} \max_{\frac{1}{2}x \leq N \leq x} \left| \psi(N+y; q, a) - \psi(N; q, a) - \frac{y}{\varphi(q)} \right| \ll \frac{h}{(\log x)^D},$$

where  $D > 0$ ,  $\delta > 0$ , and  $\theta > 0$  are constants and  $h \geq x^{1-\delta}$ . The Density Hypothesis for Dirichlet  $L$ -functions, which follows from GRH, predicts that (1.4) holds when  $0 \leq \delta < \frac{1}{2}$  and  $0 \leq \theta < \frac{1}{2} - \delta$  [9, Chapter 12]. There has been much progress toward this conjectured estimate; see [16] and the sources contained therein. Currently, the sharpest version of (1.4) is due to Timofeev [21], who proved that (1.4) holds when  $0 \leq \delta < \frac{5}{12}$  and

$$0 \leq \theta < \begin{cases} \frac{1}{2} - \delta & \text{if } 0 \leq \delta < \frac{2}{5}, \\ \frac{9}{20} - \delta & \text{if } \frac{2}{5} \leq \delta < \frac{5}{12}. \end{cases}$$

Some of these results have been extended to a Chebotarev setting. Specifically, let  $L/K$  be a Galois extension of number fields with Galois group  $G$  and absolute discriminant  $d_L$ , let  $a, q \in \mathbb{N}$  with  $(a, q) = 1$ , and let  $N = N_{K/\mathbb{Q}}$  denote the absolute field norm of  $K$ . For a prime ideal  $\mathfrak{p}$  of  $K$  which is unramified in  $L$ , there corresponds a certain conjugacy class  $C \subset G$  consisting of the set of Frobenius automorphisms attached to the prime ideals of  $L$  which lie over  $\mathfrak{p}$ . We denote this conjugacy class by the Artin symbol  $\left[\frac{L/K}{\mathfrak{p}}\right]$ .

For a fixed conjugacy class  $C$  and an integral ideal  $\mathfrak{a}$  of  $K$ , define

$$\Lambda_C(\mathfrak{a}) = \begin{cases} \log N\mathfrak{p} & \text{if } \mathfrak{a} = \mathfrak{p}^m \text{ with } m \geq 1, \mathfrak{p} \text{ unramified in } L, \text{ and } \left[\frac{L/K}{\mathfrak{p}}\right]^m = C, \\ 0 & \text{otherwise} \end{cases}$$

and

$$\psi_C(x; q, a) = \sum_{\substack{N\mathfrak{a} \leq x \\ N\mathfrak{a} \equiv a \pmod{q}}} \Lambda_C(\mathfrak{a}).$$

The Chebotarev density theorem tells us that if  $q \leq (\log x)^D$ , then

$$(1.5) \quad \psi_C(2x; q, a) - \psi_C(x; q, a) \sim d(C; q, a)x$$

for some density  $d(C; q, a) \geq 0$ . If  $(q, d_L) = 1$ , then

$$d(C; q, a) = \frac{|C|}{|G|} \frac{1}{\varphi(q)}.$$

In the case of  $q = 1$ , Balog and Ono [1] extended (1.5) to a short interval setting by proving that if we fix

$$(1.6) \quad 0 < \delta < \begin{cases} 1/[L : \mathbb{Q}] & \text{if } [L : \mathbb{Q}] \geq 3, \\ 3/8 & \text{if } [L : \mathbb{Q}] = 2, \\ 5/12 & \text{if } [L : \mathbb{Q}] = 1 \end{cases}$$

and choose  $h \geq x^{1-\delta}$ , then

$$(1.7) \quad \psi_C(x+h; 1, 1) - \psi_C(x; 1, 1) \sim \frac{|C|}{|G|} h.$$

Building on the work of M. Ram Murty and V. K. Murty [10], M. Ram Murty and Petersen [11] proved that if  $H \subset G$  is the largest abelian subgroup of  $G$  such that  $H \cap C$  is nonempty,  $E$  is the fixed field of  $H$ , and  $0 \leq \theta < 1/\max\{[E:\mathbb{Q}] - 2, 2\}$  is fixed, then

$$(1.8) \quad \sum'_{q \leq x^\theta} \max_{(a,q)=1} \max_{N \leq x} \left| \psi_C(2N; q, a) - \psi_C(N; q, a) - \frac{|C|}{|G|} \frac{N}{\varphi(q)} \right| \ll \frac{x}{(\log x)^D},$$

where  $\sum'$  denotes summing over moduli  $q$  satisfying  $(q, d_L) = 1$ . This extends (1.3) to a Chebotarev setting; in fact, (1.3) is recovered when  $L = \mathbb{Q}$ . Our main result is a Chebotarev analogue of (1.4), which we prove in Section 2.

**Theorem 1.1.** *Let  $L/K$  be a Galois extension of number fields with Galois group  $G$  and absolute discriminant  $d_L$ , and let  $C \subset G$  be a fixed conjugacy class. Let  $H \subset G$  be the largest abelian subgroup of  $G$  such that  $H \cap C$  is nonempty, and let  $E$  be the fixed field of  $H$ . Fix  $0 \leq \delta < \frac{2}{5[E:\mathbb{Q}]}$  and  $0 \leq \theta < \frac{1}{3}(\frac{2}{5[E:\mathbb{Q}]} - \delta)$ . If  $h \geq x^{1-\delta}$ , then for any fixed  $D > 0$ , we have*

$$\sum'_{q \leq x^\theta} \max_{(a,q)=1} \max_{y \leq h} \max_{\frac{1}{2}x \leq N \leq x} \left| \psi_C(N+y; q, a) - \psi_C(N; q, a) - \frac{|C|}{|G|} \frac{y}{\varphi(q)} \right| \ll \frac{h}{(\log x)^D},$$

where  $\sum'$  denotes summing over moduli  $q$  satisfying  $(q, d_L) = 1$ .

The following improvement on the range of  $\delta$  (1.6) in Balog and Ono's short interval version of the Chebotarev density theorem (1.7) follows immediately from Theorem 1.1.

**Corollary 1.2.** *Let  $L/K$  be a Galois extension of number fields with Galois group  $G$  and absolute discriminant  $d_L$ , and let  $C \subset G$  be a fixed conjugacy class. Suppose that  $[L:\mathbb{Q}] \geq 3$ . Let  $H \subset G$  be the largest abelian subgroup of  $G$  such that  $H \cap C$  is nonempty, and let  $E$  be the fixed field of  $H$ . Suppose that  $q \leq (\log x)^D$  satisfies  $(q, d_L) = 1$  and  $(a, q) = 1$ . If  $0 \leq \delta < \max\{\frac{1}{[L:\mathbb{Q}]}, \frac{2}{5[E:\mathbb{Q}]}\}$  is fixed and  $h \geq x^{1-\delta}$ , then*

$$\psi_C(x+h; q, a) - \psi_C(x; q, a) \sim \frac{|C|}{|G|} \frac{h}{\varphi(q)}.$$

Much like the results of [10, 11], nonabelian analogues of the Bombieri-Vinogradov theorem in short intervals can have interesting arithmetic consequences. In this paper, we will focus on consequences related to recent advances toward the Hardy-Littlewood prime  $k$ -tuples conjecture. For these applications, we consider a Galois extension  $L/\mathbb{Q}$  with Galois group  $G$  and absolute discriminant  $d_L$ , and we consider a fixed conjugacy class  $C \subset G$ . In this setting, a Chebotarev set takes the form

$$(1.9) \quad \mathcal{P} = \left\{ p : p \nmid d_L, \left[ \frac{L/\mathbb{Q}}{p} \right] = C \right\}$$

We establish some additional notation. Let  $\mathbb{P}$  denote the set of all primes, and let  $h_i$  denote a nonnegative integer. We call a collection of linear forms  $\mathcal{H}_k = \{n+h_1, \dots, n+h_k\}$  *admissible* if  $\prod_{i=1}^k (n+h_i)$  has no fixed prime divisor. (We could consider more general admissible sets  $\{a_1n+b_1, \dots, a_kn+b_k\}$ , but this sometimes hinders the applications we consider.)

**Conjecture** (Hardy-Littlewood). *If  $\mathcal{H}_k$  is admissible, then as  $x \rightarrow \infty$ , we have*

$$\#\{n \in [x, 2x] : \#(\{n+h_1, \dots, n+h_k\} \cap \mathbb{P}) = k\} \sim \mathfrak{S} \frac{x}{(\log x)^k},$$

where  $\mathfrak{S}$  is a certain positive constant depending on  $\mathcal{H}_k$ .

Choosing  $\mathcal{H}_2 = \{0, 2\}$ , the Hardy-Littlewood conjecture implies the elusive twin prime conjecture, that there are infinitely many pairs of primes whose difference is 2.

In [8], Maynard developed a significant improvement to the Selberg sieve. By using this improvement in conjunction with (1.3), Maynard proved that if  $\mathcal{H}_k$  is admissible, then there are infinitely many integers  $N > 0$  such that for some  $n \in [N, 2N]$ , we have

$$\#(\{n + h_1, \dots, n + h_k\} \cap \mathbb{P}) \geq (1/4 + o_{k \rightarrow \infty}(1)) \log k.$$

(Tao independently derived the same improvement as Maynard at roughly the same time, but arrived at slightly different conclusions.) Using (1.8) and Maynard's improvement to the Selberg sieve, the author [20] proved that if  $\mathcal{H}_k$  is admissible, then there are infinitely many integers  $N > 0$  such that for some  $n \in [N, 2N]$ , we have

$$\#(\{n + h_1, \dots, n + h_k\} \cap \mathcal{P}) \geq \left( \frac{1}{2} \min \left\{ \frac{1}{2}, \frac{2}{|G|} \right\} \frac{|C|}{|G|} \frac{\varphi(d_L)}{d_L} + o_{k \rightarrow \infty}(1) \right) \log k,$$

where  $\mathcal{P}$  is a Chebotarev set given by (1.9). The author explored applications of this result to ranks of quadratic twists of elliptic curves, congruence conditions on the Fourier coefficients of newforms, and representations of primes by binary quadratic forms.

In [7], Maynard generalized his methods to prove weak forms of the Hardy-Littlewood conjecture with specializations to primes in short intervals and primes in Chebotarev sets. More specifically, given  $0 \leq \delta < \frac{5}{12}$  and  $h \geq x^{1-\delta}$ , Maynard proved that there exists an absolute constant  $C > 0$  such that if  $k \geq C$  and  $\mathcal{H}_k$  is an admissible set, then

$$(1.10) \quad \#\{n \in [x, x+h] : \#(\{n + h_1, \dots, n + h_k\} \cap \mathbb{P}) \geq C^{-1} \log k\} \gg \frac{h}{(\log x)^k}$$

Furthermore, if  $\mathcal{P}$  is given by (1.9), then Maynard also proved that there exists a constant  $C_L > 0$  such that if  $k \geq C_L$  and  $\mathcal{H}_k$  is admissible, then

$$(1.11) \quad \#\{n \in [x, 2x] : \#(\{n + h_1, \dots, n + h_k\} \cap \mathcal{P}) \geq C_L^{-1} \log k\} \gg \frac{x}{(\log x)^k}.$$

(The subscript  $L$  in  $C_L$  denotes that the constant  $C$  depends only on  $L$  in an effectively computable fashion. We will use this convention henceforth.)

Using Theorem 1.1, we prove in Section 3 the following mutual refinement of (1.10) and (1.11), which extends the author's applications in [20] to a short interval setting.

**Theorem 1.3.** *Let  $L/\mathbb{Q}$  be a Galois extension of number fields, let  $\mathcal{P}$  be as in (1.9), and choose  $h$  as in Theorem 1.1. There exists a constant  $C_L \in \mathbb{N}$  such that if  $k \geq C_L$  and  $\mathcal{H}_k$  is admissible, then*

$$\#\{n \in [x, x+h] : \#(\{n + h_1, \dots, n + h_k\} \cap \mathcal{P}) \geq C_L^{-1} \log k\} \gg \frac{h}{(\log x)^k}.$$

*Remark.* Some of the parameters in the statement of Theorem 1.3 can have some uniformity in  $x$  by appealing to the arguments in [7]. In what follows, all parameters are constant with respect to  $x$ .

We now consider arithmetic consequences of Theorem 1.3 in the theory of elliptic curves, modular forms, and modular  $L$ -functions; for an introduction to the relevant definitions and ideas, we refer the reader to [14]. We consider the following question of Serre [17], which

may be seen as an automorphic analogue of Bertrand's postulate on the existence of primes in every dyadic interval  $[x, 2x]$ .

**Serre's Question.** *Let  $q = e^{2\pi iz}$ , and let  $S_\ell(\Gamma_0(N), \chi)$  denote the space of weight  $\ell$ , level  $N$  cusp forms. For a nonzero cusp form  $f(z) = \sum_{n=1}^{\infty} a_f(n)q^n \in S_\ell(\Gamma_0(N), \chi)$ , let*

$$I_f(n) = \max\{i : a_f(n+j) = 0 \text{ for all } 0 \leq j \leq i\}.$$

- (1) *Suppose that  $f$  is of weight  $\ell \geq 2$  and is not a linear combination of forms with complex multiplication. Is  $I_f(n) \ll n^\delta$  for some  $0 \leq \delta < 1$ ?*
- (2) *More generally, are there analogous results for forms with non-integral weights, or forms with respect to other Fuchsian groups?*

Motivated by the second part of Serre's question, Balog and Ono [1] used (1.7) to prove that if  $f(z) = \sum_{n=1}^{\infty} a_f(n)q^n \in S_\ell(\Gamma_0(N), \chi)$  is a cusp form of weight  $\ell \in \frac{1}{2}\mathbb{N} - \{\frac{1}{2}\}$  which is not a linear combination of weight  $\frac{3}{2}$  theta functions, then there exists  $\nu_f \in \mathbb{N}$  such that if  $0 \leq \delta < \frac{1}{\nu_f}$  and  $h \geq x^{1-\delta}$ , then

$$(1.12) \quad \#\{n \in [x, x+h] : a_f(n) \neq 0\} \gg \frac{h}{\log x}.$$

For such a cusp form  $f$ , it follows that  $I_f(n) \ll n^{1-\frac{1}{\nu_f}+\epsilon}$  for any  $\epsilon > 0$ , affirmatively answering Serre's question. By using Theorem 1.3 instead of (1.7) in Balog and Ono's proof, we immediately obtain dense clusters of integers  $n$  in short intervals for which  $a_f(n) \neq 0$ . Specifically, we have the following.

**Theorem 1.4.** *Let  $f(z) = \sum_{n=1}^{\infty} a_f(n)q^n \in S_\ell(\Gamma_0(N), \chi)$  be a nonzero cusp form of weight  $\ell \in \frac{1}{2}\mathbb{N} - \{\frac{1}{2}\}$  which is not a linear combination of weight  $\frac{3}{2}$  theta functions. There exist constants  $C_f, \nu_f \in \mathbb{N}$  such that if  $0 \leq \delta < \frac{1}{\nu_f}$ ,  $h \geq x^{1-\delta}$ ,  $k \geq C_f$  and  $\mathcal{H}_k$  is admissible, then*

$$\#\{n \in [x, x+h] : \#\{h_i \in \mathcal{H}_k : a_f(n+h_i) \neq 0\} \geq C_f^{-1} \log k\} \gg \frac{h}{(\log x)^k}.$$

We address two corollaries of Theorem 1.4 regarding central values of modular  $L$ -functions and ranks of elliptic curves. Let  $\mathcal{D}$  be the set of all fundamental discriminants, and let  $f(z) = \sum_{n=1}^{\infty} a_f(n)q^n \in S_\ell(\Gamma_0(N))$  be a newform (i.e., a holomorphic cuspidal normalized Hecke eigenform) of weight  $\ell \in 2\mathbb{N}$ . Given  $d \in \mathcal{D}$ , let  $L(s, f_d)$  denote the  $L$ -function given by

$$L(s, f_d) = \sum_{n=1}^{\infty} \frac{a_f(n)\chi_d(n)}{n^{s+(\ell-1)/2}},$$

where  $\chi_d$  is the Kronecker character for  $\mathbb{Q}(\sqrt{d})$ . Goldfeld [4] conjectured that the density of  $d \in \mathcal{D}$  for which  $L(1/2, f_d) \neq 0$  is  $1/2$ .

By the work of Shimura [18] and Waldspurger [22], Fourier coefficients of half-integer weight cusp forms  $g$  that satisfy the hypotheses of Theorem 1.4 interpolate central values of quadratic twists of modular  $L$ -functions associated to the Shimura correspondent of  $g$ . Despite the fact that the Shimura correspondence is not surjective, Ono and Skinner [15] proved that such central values can be obtained in this fashion for the  $L$ -function of an even-integer weight newform with trivial nebentypus. Using this observation along with (1.12),

Balog and Ono [1] proved that there exists  $\nu_F \in \mathbb{N}$  such that if  $0 \leq \delta < \frac{1}{\nu_F}$  and  $h \geq x^{1-\delta}$ , then

$$(1.13) \quad \#\{|d| \in [x, x+h] : d \in \mathcal{D}, L(1/2, f_d) \neq 0\} \gg \frac{h}{\log x}.$$

This is the sharpest result in the direction of Goldfeld's conjecture which is valid for all newforms  $f$ ; slight improvements exist for certain classes of newforms [13]. By using Theorem 1.4 instead of (1.12) in Balog and Ono's proof, we immediately obtain dense clusters of fundamental discriminants  $d$  in short intervals for which  $L(1/2, f_d) \neq 0$ .

**Corollary 1.5.** *Let  $f \in S_{2\ell}(\Gamma_0(N))$  be a newform with  $\ell \in \mathbb{N}$ . There exists an arithmetic progression  $a \bmod q$  (which depends explicitly on  $f$ ) and constants  $\nu_f, C_f \in \mathbb{N}$  such that if  $0 \leq \delta < \frac{1}{\nu_f}$ ,  $h \geq x^{1-\delta}$ ,  $k \geq C_f$ ,  $\mathcal{H}_k$  is admissible, and*

$$\mathcal{N}_f(k, n) = \{h_i \in \mathcal{H}_k : n + qh_i \in \mathcal{D}, L(1/2, f_{n+qh_i}) \neq 0\},$$

then

$$\#\{|n| \in [x, x+h] : n \equiv a \pmod{q}, \#\mathcal{N}_f(k, n) \geq C_f^{-1} \log k\} \gg \frac{h}{(\log x)^k}.$$

*Remark.* We need to restrict to the arithmetic progression  $a \bmod q$  for technical reasons; see [15] for details. We accomplish this by combining the arguments of Freiburg [3, Proof of Theorem 1] with Maynard's proofs in [7], which is fairly straightforward.

Let  $f$  be the newform associated to an elliptic curve  $E/\mathbb{Q}$  of conductor  $N$ . If  $(d, 4N) = 1$ , then  $L(s, f_d)$  is the  $L$ -function of the  $d$ -quadratic twist  $E_d/\mathbb{Q}$ . By the work of Kolyvagin [6], if  $L(1/2, f_d) \neq 0$ , then the rank  $\text{rk}(E_d(\mathbb{Q}))$  of the Mordell-Weil group  $E_d(\mathbb{Q})$  is zero. Thus Corollary 1.5 immediately implies the existence of dense clusters of fundamental discriminants  $d$  in short intervals such that  $\text{rk}(E_d) = 0$ .

**Corollary 1.6.** *Let  $E/\mathbb{Q}$  be an elliptic curve. There exist an arithmetic progression  $a \bmod q$  (which depends explicitly on  $E$ ) and constants  $\nu_E, C_E \in \mathbb{N}$  such that if  $0 \leq \delta < \frac{1}{\nu_E}$ ,  $h \geq x^{1-\delta}$ ,  $k \geq C_E$ ,  $\mathcal{H}_k$  is admissible, and*

$$\mathcal{N}_E(k, n) = \{h_i \in \mathcal{H}_k : n + qh_i \in \mathcal{D}, \text{rk}(E_{n+qh_i}) = 0\},$$

then

$$\#\{|n| \in [x, x+h] : n \equiv a \pmod{q}, \#\mathcal{N}_E(k, n) \geq C_E^{-1} \log k\} \gg \frac{h}{(\log x)^k}.$$

For our final application, consider an elliptic curve  $E/\mathbb{Q}$ . In [12, 17], the distribution of the quantity  $a_E(p) := p + 1 - \#E(\mathbb{F}_p)$  is studied. We apply our results to study the distribution of  $a_E(p) \pmod{m}$  in short intervals, where  $m$  is a given integer. It follows from the work of Shiu [19] that if  $E/\mathbb{Q}$  has a rational point of order  $m$ , then for every  $j \in \mathbb{N}$  and every  $i \not\equiv 1 \pmod{m}$ , there exists an  $n \in \mathbb{N}$  such that

$$a_E(p_n) \equiv a_E(p_{n+1}) \equiv a_E(p_{n+2}) \equiv \cdots \equiv a_E(p_{n+j}) \equiv i \pmod{m},$$

where the primes are indexed in increasing order. Using (1.7) and the definition of the action of Galois on the torsion points of  $E$ , Balog and Ono [1] proved that if  $m \in \mathbb{N}$  and  $i \bmod m$

is a residue class for which there is a prime of good reduction  $p_0$  with  $a_E(p_0) \equiv i \pmod{m}$ , then there exists  $\nu_{E,m} \in \mathbb{N}$  such that if  $0 \leq \delta < \frac{1}{\nu_{E,m}}$  and  $h \geq x^{1-\delta}$ , then

$$(1.14) \quad \#\{p \in [x, x+h] : a_E(p) \equiv i \pmod{m}\} \gg \frac{h}{\log x}.$$

By using Theorem 1.3 instead of (1.7) in Balog and Ono's proof, we immediately obtain dense clusters of primes  $p$  in short intervals for which  $a_E(p) \equiv i \pmod{m}$ .

**Corollary 1.7.** *Let  $E/\mathbb{Q}$  be an elliptic curve, let  $m \in \mathbb{N}$ , and let  $i \pmod{m}$  be a residue class for which there is a prime of good reduction  $p_0$  with  $a_E(p_0) \equiv i \pmod{m}$ . There exist constants  $\nu_{E,m}, C_{E,m} \in \mathbb{N}$  such that if  $0 \leq \delta < \frac{1}{\nu_{E,m}}$ ,  $h \geq x^{1-\delta}$ ,  $k \geq C_{E,m}$ , and  $\mathcal{H}_k$  is admissible, then*

$$\begin{aligned} & \#\{n \in [x, x+h] : \#\{h_j \in \mathcal{H}_k : n+h_j \in \mathbb{P}, a_E(n+h_j) \equiv i \pmod{m}\} \geq C_{E,m}^{-1} \log k\} \\ & \gg \frac{h}{(\log x)^k}. \end{aligned}$$

## ACKNOWLEDGMENTS

The author thanks James Maynard, Robert Lemke Oliver, Ken Ono, Jeremy Rouse, Kannan Soundararajan, and the anonymous referees for their comments and suggestions.

## 2. PROOF OF THEOREM 1.1

For a number field  $F$ , we let  $n_F = [F : \mathbb{Q}]$  and  $d_F$  equal the absolute discriminant of  $F$ . Let  $L/K$  be a Galois extension of number fields with Galois group  $G$ , and let  $C \subset G$  be a fixed conjugacy class. Let  $H$  be the largest abelian subgroup of  $G$  such that  $H \cap C$  is nonempty, and let  $E$  be the field fixed by  $H$ . If  $L \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}$ , then  $L(\zeta_q)/E$  is an abelian extension with Galois group  $H_q$ , which is isomorphic to  $H \oplus (\mathbb{Z}/q\mathbb{Z})^\times$ . Let  $\chi$  be a Dirichlet character modulo  $q$ , and let  $\xi$  be a Hecke character in the dual group  $\hat{H}$ . Since  $L \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}$ , the characters  $\omega$  in the dual group  $\hat{H}_q$  are of the form  $\xi \otimes \chi$ , and the conductor  $\mathfrak{f}_\omega$  of  $\omega$  satisfies  $N\mathfrak{f}_\omega \leq q^{n_K} N\mathfrak{f}_\xi$ , where  $N$  is the absolute field norm of  $E$  (cf. [11, Sections 0 and 1]). Unless otherwise specified, all implied constants in the asymptotic notation  $\ll$  or  $O(\cdot)$  will depend in an effectively computable way on at most  $\max_{\xi \in \hat{H}} N\mathfrak{f}_\xi$ .

By Equation 3.2 of [1] and the functional equation for Hecke  $L$ -functions, if  $y \leq h$ ,  $\frac{1}{2}x \leq N \leq x$ , and  $T \leq x$ , then

$$\begin{aligned} & \max_{y \leq h} \max_{\frac{1}{2}x \leq N \leq x} \left| \psi_C(N+y; q, a) - \psi_C(N; q, a) - \frac{|C|}{|G|} \frac{y}{\varphi(q)} \right| \\ & \ll \frac{h}{\varphi(q)} \sum_{\omega \in \hat{H}_q} \sum_{\substack{\rho = \beta + i\gamma \\ L(\rho, \tilde{\omega}) = 0 \\ |\gamma| \leq T \\ \frac{1}{2} \leq \beta < 1}} x^{\beta-1} + \frac{x(\log x)^2}{T}, \end{aligned}$$



where  $\tilde{\omega}$  is the primitive character which induces  $\omega$ . Thus Theorem 1.1 will follow from proving that for any fixed  $D > 0$ , we have that

$$(2.1) \quad h \sum'_{q \leq Q} \frac{1}{\varphi(q)} \sum_{\omega \in \hat{H}_q}^* \sum_{\substack{\rho_\omega = \beta_\omega + i\gamma_\omega \\ \frac{1}{2} \leq \beta_\omega < 1 \\ |\gamma_\omega| \leq T}} x^{\beta_\omega - 1} + \frac{Qx(\log x)^2}{T} \ll \frac{h}{(\log x)^D},$$

where  $\rho_\omega$  is a nontrivial zero of  $L(s, \omega)$  and  $\sum^*$  denotes summing over primitive characters  $\omega$ . (See also [11, Section 1] for a similar reduction.) We now decompose the interval  $[1, Q]$  into dyadic intervals of the form  $[2^n, 2^{n+1})$ , where  $0 \leq n \leq \lceil \log_2 Q \rceil$ . Since there are  $O(\log Q)$  such intervals and  $\varphi(q)^{-1} \ll q^{-1} \log \log q$  for  $q \geq 6$ , the left side of (2.1) is

$$(2.2) \quad (\log Q)(\log \log Q) \max_{1 \leq Q_1 \leq Q} \frac{1}{Q_1} \sum'_{q \leq Q_1} \sum_{\omega \in \hat{H}_q}^* \sum_{\substack{\rho_\omega = \beta_\omega + i\gamma_\omega \\ \frac{1}{2} \leq \beta_\omega < 1 \\ |\gamma_\omega| \leq T}} x^{\beta_\omega - 1} + \frac{Qx(\log x)^2}{T}.$$

If  $\omega$  is primitive, then  $\mathfrak{f}_\omega$  is also the modulus of  $\omega$ . Since  $N\mathfrak{f}_\omega \leq q^{n_E} \max_{\xi \in \hat{H}} N\mathfrak{f}_\xi$ , (2.2) is

$$(2.3) \quad \ll (\log Q)(\log \log Q) \max_{1 \leq Q_1 \leq Q} \frac{1}{Q_1} \sum_{N\mathfrak{a} \leq Q_1^{n_E}} \sum_{\omega \bmod \mathfrak{a}}^* \sum_{\substack{\rho_\omega = \beta_\omega + i\gamma_\omega \\ \frac{1}{2} \leq \beta_\omega < 1 \\ |\gamma_\omega| \leq T}} x^{\beta_\omega - 1} + \frac{Qx(\log x)^2}{T}.$$

For  $\frac{1}{2} \leq \sigma \leq 1$ , let  $N_\omega(\sigma, T) := \#\{\rho = \beta + i\gamma : L(\rho, \omega) = 0, \sigma \leq \beta, |\gamma| \leq T\}$  and

$$N(\sigma, R, T) := \sum_{N\mathfrak{a} \leq R} \sum_{\omega \bmod \mathfrak{a}}^* N_\omega(\sigma, T).$$

Building on the seminal work of Montgomery [9, Theorem 12.2], Hinz [5] proved estimates for  $N(\sigma, Q^{n_E}, T)$  when  $n_E \geq 2$ . The following proposition is a direct corollary of their combined work.

**Proposition 2.1.** *If  $T \geq 2$ ,  $R \geq 1$ , and  $\frac{1}{2} \leq \sigma \leq 1$ , then*

$$N(\sigma, R, T) \ll (R^2 T^{n_E})^{\frac{5}{2}(1-\sigma)} (\log QT)^{9n_E+10}.$$

*Proof of Theorem 1.1.* Let  $D, \delta$ , and  $h$  be as in the statement of Theorem 1.1. Let  $0 < \epsilon < 1$ , and choose  $Q = x^{\frac{2(1-\epsilon)-5n_E\delta}{15n_E}} (\log x)^{-\frac{D+2}{3}}$  and  $T = x^{\frac{2(1-\epsilon+5n_E\delta)}{15n_E}} (\log x)^{\frac{2(D+2)}{3}}$ . With  $1 \leq Q_1 \leq Q$ , we have

$$(2.4) \quad \sum_{N\mathfrak{a} \leq Q_1^{n_E}} \sum_{\omega \bmod \mathfrak{a}}^* \sum_{\substack{\rho_\omega = \beta_\omega + i\gamma_\omega \\ \frac{1}{2} \leq \beta_\omega < 1 \\ |\gamma_\omega| \leq T}} x^{\beta_\omega - 1} \ll \log x \max_{\frac{1}{2} \leq \sigma < 1} x^{\sigma-1} N(\sigma, Q_1^{n_E}, T).$$

By the zero-free region for Hecke  $L$ -functions proven by Bartz [2] and the fact that we restrict  $q$  so that  $L \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}$ , there exists a constant  $b_L > 0$  such that if

$$(2.5) \quad 1 - \eta(Q_1, x) < \sigma \leq 1, \quad \eta(Q_1, x) := \frac{b_L}{\max\{\log Q_1, (\log x)^{3/4}\}},$$

then  $N(\sigma, Q_1^{n_E}, T)$  is either 0 or 1. If  $N(\sigma, Q_1^{n_E}, T) = 1$ , then the zero  $\beta_1$  which is counted is a Siegel zero associated to an exceptional modulus  $q_1$  and an exceptional real quadratic



character in  $\widehat{H}_{q_1}$ . As in [11, Section 2], a field-uniform version of Siegel's theorem for Hecke  $L$ -functions implies that  $x^{\beta_1-1} \ll (\log x)^{-D-3}$  with an ineffective implied constant.

Since  $(Q^2 T)^{\frac{5}{2}n_E} = x^{1-\epsilon}$ , it follows from Proposition 2.1 that

$$\begin{aligned} \log x \max_{\frac{1}{2} \leq \sigma \leq 1-\eta(Q_1, T)} x^{\sigma-1} N(\sigma, Q_1^{n_E}, T) &\ll (\log x)^{9n_E+11} \max_{\frac{1}{2} \leq \sigma \leq 1-\eta(Q_1, T)} ((Q^2 T)^{\frac{5}{2}n_E} / x)^{1-\sigma} \\ &\ll (\log x)^{9n_E+11} x^{-\epsilon\eta(Q_1, x)}. \end{aligned}$$

By our definition of  $\eta(Q_1, x)$ ,

$$(2.6) \quad x^{-\epsilon\eta(Q_1, x)} \ll \begin{cases} (\log x)^{-(9n_E+14+D)} & \text{if } 1 \leq Q_1 \leq \exp((\log x)^{3/4}), \\ 1 & \text{if } \exp((\log x)^{3/4}) < Q_1 \leq Q. \end{cases}$$

We have now bounded (2.4), and so (2.3) is bounded by

$$h(\log Q)(\log \log Q)(\log x) \max_{Q_1 \leq Q} \frac{1}{Q_1} ((\log x)^{-D-3} + (\log x)^{9n_E+11} x^{-\epsilon\eta(Q_1, x)}) + \frac{Qx(\log x)^2}{T}.$$

For our choice of  $h$ ,  $Q$ , and  $T$ , this is bounded by  $h(\log x)^{-D}$  using (2.6).  $\square$

### 3. PROOF OF THEOREM 1.3

We will use Theorem 1.1 to prove Theorem 1.3. Given a set of integers  $\mathfrak{A}$ , a set of primes  $\mathfrak{P} \subset \mathfrak{A}$ , and a linear form  $L(n) = n + h$ , define

$$\begin{aligned} \mathfrak{A}(x) &= \{n \in \mathfrak{A} : x < n \leq 2x\}, & \mathfrak{A}(x; q, a) &= \{n \in \mathfrak{A}(x) : n \equiv a \pmod{q}\}, \\ L(\mathfrak{A}) &= \{L(n) : n \in \mathfrak{A}\}, & \varphi_L(q) &= \varphi(hq)/\varphi(h), \\ \mathfrak{P}_{L, \mathfrak{A}}(x, y) &= L(\mathfrak{A}(x)) \cap \mathfrak{P}, & \mathfrak{P}_{L, \mathfrak{A}}(x; q, a) &= L(\mathfrak{A}(x; q, a)) \cap \mathfrak{P}. \end{aligned}$$

We consider the 6-tuple  $(\mathfrak{A}, \mathcal{L}_k, \mathfrak{P}, B, x, \theta)$ , where  $\mathcal{H}_k$  is admissible,  $\mathcal{L}_k = \{L_i(n) = n + h_i : h_i \in \mathcal{H}_k\}$ ,  $B \in \mathbb{N}$  is constant,  $x$  is a large real number, and  $0 \leq \theta < 1$ . We present a very general hypothesis that Maynard states in Section 2 of [7].

**Hypothesis 3.1.** *With the above notation, consider the 6-tuple  $(\mathfrak{A}, \mathcal{H}_k, \mathfrak{P}, B, x, \theta)$ .*

(1) *We have*

$$\sum_{q \leq x^\theta} \max_a \left| \#\mathfrak{A}(x; q, a) - \frac{\#\mathfrak{A}(x)}{q} \right| \ll \frac{\#\mathfrak{A}(x)}{(\log x)^{100k^2}}.$$

(2) *For any  $L \in \mathcal{H}_k$ , we have*

$$\sum_{\substack{q \leq x^\theta \\ (q, B)=1}} \max_{(L(a), q)=1} \left| \#\mathfrak{P}_{L, \mathfrak{A}}(x; q, a) - \frac{\#\mathfrak{P}_{L, \mathfrak{A}}(x)}{\varphi_L(q)} \right| \ll \frac{\#\mathfrak{P}_{L, \mathfrak{A}}(x)}{(\log x)^{100k^2}}.$$

(3) *For any  $q \leq x^\theta$ , we have  $\#\mathfrak{A}(x; q, a) \ll \#\mathfrak{A}(x)/q$ .*

For  $(\mathfrak{A}, \mathcal{H}_k, \mathfrak{P}, B, x, \theta)$  satisfying Hypothesis 3.1, Maynard proves the following in [7].

**Theorem 3.2.** *Let  $\alpha > 0$  and  $0 \leq \theta < 1$ . There is a constant  $C$  depending only on  $\theta$  and  $\alpha$  so that the following holds. Let  $(\mathfrak{A}, \mathcal{H}_k, \mathfrak{P}, B, x, \theta)$  satisfy Hypothesis 3.1. Assume that  $C \leq k \leq (\log x)^\alpha$  and  $h_i \leq x^\alpha$  for all  $1 \leq i \leq k$ . If  $\delta > (\log k)^{-1}$  is such that*

$$\frac{1}{k} \frac{\varphi(B)}{B} \sum_{L_i \in \mathcal{H}_k} \#\mathfrak{P}_{L_i, \mathfrak{A}}(x) \geq \delta \frac{\#\mathfrak{A}(x)}{\log x},$$

*then*

$$\#\{n \in \mathfrak{A}(x) : \#(\mathcal{H}_k(n) \cap \mathfrak{P}) \geq C^{-1} \delta \log k\} \gg \frac{\#\mathfrak{A}(x)}{(\log x)^k \exp(Ck)}.$$

*Proof of Theorem 1.3.* The proof is essentially the same as Theorems 3.4 and 3.5 in [7]. Let  $\delta$ ,  $h$ , and  $\theta$  be as in Theorem 1.1. Let  $\mathfrak{A} = \mathbb{N} \cap [x, x+h]$ ,  $B = d_L$ , and  $\mathfrak{P} = \mathcal{P}$ . Parts (i) and (iii) of Hypothesis 3.1 are trivial to check for the 6-tuple  $(\mathbb{N} \cap [x, x+h], \mathcal{H}_k, \mathcal{P}, d_L, x, \theta/2)$ . By Theorem 1.1 and partial summation, all of Hypothesis 3.1 holds when  $D$  and  $x$  are sufficiently large in terms of  $k$  and  $\theta$ . Given a suitable constant  $C_L > 0$  (computed as in [8, 20]), we let  $k \geq C_L$ . For our choice of  $\mathfrak{A}$  and  $\mathfrak{P}$ , we have the inequality

$$\frac{1}{k} \frac{\varphi(d_L)}{d_L} \sum_{L_i \in \mathcal{H}_k} \#\mathfrak{P}_{L_i, \mathfrak{A}}(x) \geq (1 + o(1)) \frac{\varphi(d_L)}{d_L} \frac{|C|}{|G|} \frac{\#\mathfrak{A}(x)}{\log x}$$

for all sufficiently large  $x$ , where the implied constant in  $1 + o(1)$  depends only on  $L$ . Theorem 1.3 now follows directly from Theorem 3.2.  $\square$

## REFERENCES

- [1] A. Balog and K. Ono, *The Chebotarev density theorem in short intervals and some questions of Serre*, J. Number Theory **91** (2001), no. 2, 356–371.
- [2] K. M. Bartz, *An effective order of Hecke-Landau zeta functions near the line  $\sigma = 1$ . II. (Some applications)*, Acta Arith. **52** (1989), no. 2, 163–170.
- [3] T. Freiburg, *A note on the theorem of Maynard and Tao*, Advances in the Theory of Numbers (to appear).
- [4] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979), 1979, pp. 108–118.
- [5] J. Hinz, *Über Nullstellen der Heckschen Zetafunktionen in algebraischen Zahlkörpern*, Acta Arith. **31** (1976), no. 2, 167–193.
- [6] V. A. Kolyvagin, *Finiteness of  $E(\mathbf{Q})$  and  $SH(E, \mathbf{Q})$  for a subclass of Weil curves*, Izv. Akad. Nauk SSSR Ser. Mat. **52** (1988), no. 3, 522–540, 670–671.
- [7] J. Maynard, *Dense clusters of primes in subsets*, arxiv.org/abs/1405.2593.
- [8] ———, *Small gaps between primes*, Ann. of Math. (2) **181** (2015), no. 1, 383–413.
- [9] H. L. Montgomery, *Topics in multiplicative number theory*, Lecture Notes in Mathematics, Vol. 227, Springer-Verlag, Berlin-New York, 1971.
- [10] M. Ram Murty and V. Kumar Murty, *A variant of the Bombieri-Vinogradov theorem*, Number theory (Montreal, Que., 1985), 1987, pp. 243–272.
- [11] M. Ram Murty and K. L. Petersen, *A Bombieri-Vinogradov theorem for all number fields*, Trans. Amer. Math. Soc. **365** (2013), no. 9, 4987–5032.
- [12] V. Kumar Murty, *Modular forms and the Chebotarev density theorem. II*, Analytic number theory (Kyoto, 1996), 1997, pp. 287–308.
- [13] K. Ono, *Nonvanishing of quadratic twists of modular  $L$ -functions and applications to elliptic curves*, J. Reine Angew. Math. **533** (2001), 81–97.
- [14] ———, *The web of modularity: arithmetic of the coefficients of modular forms and  $q$ -series*, CBMS Regional Conference Series in Mathematics, vol. 102, Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 2004.

- [15] K. Ono and C. Skinner, *Non-vanishing of quadratic twists of modular  $L$ -functions*, Invent. Math. **134** (1998), no. 3, 651–660.
- [16] A. Perelli, J. Pintz, and S. Salerno, *Bombieri’s theorem in short intervals*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **11** (1984), no. 4, 529–539.
- [17] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. **54** (1981), 323–401.
- [18] G. Shimura, *On modular forms of half integral weight*, Ann. of Math. (2) **97** (1973), 440–481.
- [19] D. K. L. Shiu, *Strings of congruent primes*, J. London Math. Soc. (2) **61** (2000), no. 2, 359–373.
- [20] J. Thorner, *Bounded gaps between primes in Chebotarev sets*, Res. Math. Sci. **1** (2014), Art. 4, 16.
- [21] N. M. Timofeev, *Distribution of arithmetic functions in short intervals in the mean with respect to progressions*, Izv. Akad. Nauk SSSR Ser. Mat. **51** (1987), no. 2, 341–362, 447.
- [22] J.-L. Waldspurger, *Sur les coefficients de Fourier des formes modulaires de poids demi-entier*, J. Math. Pures Appl. (9) **60** (1981), no. 4, 375–484.